Summary Final Decision Art 60

Investigation

Imposition of a fine

Background information

Date of final decision:	16 May 2019
LSA:	LT
CSAs:	LV
Legal Reference:	Principles relating to processing of personal data (Article 5), Lawfulness of processing (Article 6), Information to be provided where personal data have not been obtained from the data subject (Article 14), Responsibility of the controller (Article 24), Security of processing (Article 32), Notification of a personal data breach to the supervisory authority (Article 33), General conditions for imposing administrative fines (Article 83).
Decision:	Imposition of fine
Key words:	Data breach, unlawful processing, security of the processing

Summary of the Decision

Origin of the case

This case concerned the taking of screenshots by the data controller when a user made an online payment using its service. The user, however, was not notified about the screenshots being taken. The screenshots recorded personal data of the payer, such as their name and surname, numbers, recent transactions, loans, amounts, mortgages, etc. Moreover, the data controller had provided access to individuals that were not authorised for that purpose and did not report the relevant data breach.

Findings

Regarding the processing of personal data in screenshots: The LSA considered that the processing of the personal data by the controller was beyond what is necessary for the performance of the payment service, and was also stored for a longer period that necessary. The controller failed to demonstrate the need to collect such amount of personal data. Thus, the processing violates the

data minimisation and the storage limitation principles. Moreover, users are not informed of the processing. Therefore, the LSA considers that the processing of personal data is deemed as unlawful.

Regarding the publicity of the personal data: Due to a security breach, unauthorised individuals had access to the data concerned, since access could be gained on the controller's website merely by using the ID of the transaction number. The LSA found that the controller failed to implement the appropriate technical or organisational measures to ensure data security.

Regarding the notification of the personal data breach: The data controller failed to notify the relevant data breach as required by Art. 33 of the GDPR without providing a sufficient explanation of that failure to notify.

Decision

The LSA decided to impose a fine of 61.500 €(2,5% of the controller's total annual worldwide turnover).

Comments

This is the first fine issued by this SA under OSS mechanism.